

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-250192  
(43)Date of publication of application : 17.09.1999

(51)Int.Cl. G06K 17/00  
G06F 9/06  
G06F 12/14  
G11B 7/24  
G11B 19/04

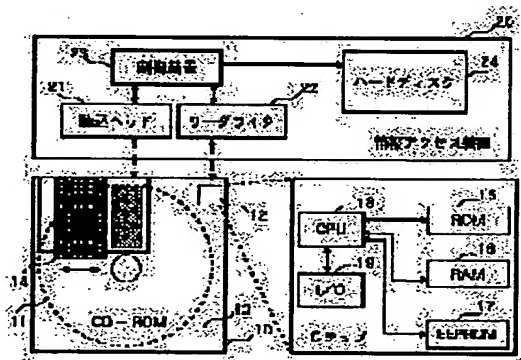
(21)Application number : 10-050713 (71)Applicant : NTT DATA CORP  
(22)Date of filing : 03.03.1998 (72)Inventor : ICHIHARA NAOHISA  
OKUMA YOSHIYUKI

## (54) RECORDING MEDIUM WITH BUILT-IN IC CHIP AND INFORMATION ACCESS CONTROLLER

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a recording medium provided with a built-in IC chip and capable of holding security for digital information such as software to be recorded.

**SOLUTION:** The recording medium 10 is constituted of housing a recording medium 11 such as a CD-ROM in a casing 13 having a shape to be housed in an information access device 20 and fitting an IC chip 12 to a prescribed position of the casing 13. A ciphered file obtained by ciphering digital information is recorded in the recording medium 11. At the time of accessing information by the device 20, the IC chip 12 executes verification, and when the verified result is affirmative, sends a decipher key for deciphering the ciphered file to the device 20. The device 20 receives the decipher key from the IC chip 12, decipheres the ciphered file and installs the deciphered file.



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平11-250192

(43)公開日 平成11年(1999) 9月17日

(51)Int.Cl.<sup>6</sup>

識別記号

F I

G 0 6 K 17/00

G 0 6 K 17/00

B

E

G 0 6 F 9/06

5 5 0

G 0 6 F 9/06

5 5 0 L

5 5 0 A

12/14

3 2 0

12/14

3 2 0 F

審査請求 未請求 請求項の数10 OL (全 7 頁) 最終頁に続く

(21)出願番号

特願平10-50713

(22)出願日

平成10年(1998) 3月3日

(71)出願人 000102728

株式会社エヌ・ティ・ティ・データ  
東京都江東区豊洲三丁目3番3号

(72)発明者 市原 尚久

東京都江東区豊洲三丁目3番3号 エヌ・  
ティ・ティ・データ通信株式会社内

(72)発明者 大熊 善之

東京都江東区豊洲三丁目3番3号 エヌ・  
ティ・ティ・データ通信株式会社内

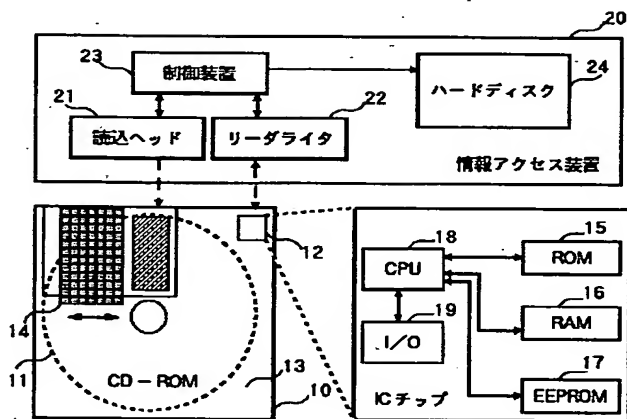
(74)代理人 弁理士 鈴木 正剛

(54)【発明の名称】 ICチップ内蔵記録媒体、情報アクセス制御装置

(57)【要約】

【課題】 記録されるソフトウェア等のデジタル情報に対するセキュリティを確保できるICチップ内蔵記録媒体を提供する。

【解決手段】 本発明のICチップ内蔵記録媒体10は、情報アクセス装置20に收容可能な形状の筐体13の内部にCD-ROM等の記録媒体11を收容するとともに筐体13の所定部位にICチップ12を取り付けて構成される。記録媒体11には、デジタル情報を暗号化した暗号化ファイルを記録しておく。ICチップ12は、情報アクセス装置20による情報アクセスの際に認証を行い、肯定的であった場合は、上記暗号化ファイルを復号化させるための復号鍵を情報アクセス装置20に送る。情報アクセス装置20は、ICチップ12から復号鍵を受け取って暗号化ファイルを復号し、インストールを行う。



## 【特許請求の範囲】

【請求項 1】 記録媒体に記録されたデジタル情報の読み取り及び IC チップへの情報アクセスとを行う装置に収容可能な形状の筐体を有し、

該筐体の内部には前記記録媒体が収容され、該筐体の所定部位には前記 IC チップが取り付けられており、前記 IC チップが、前記装置による前記デジタル情報の読み取りを規制するように構成されていることを特徴とする、IC チップ内蔵記録媒体。

【請求項 2】 前記デジタル情報が暗号化されたデジタル情報であり、  
前記 IC チップは、前記暗号化されたデジタル情報の復号化に用いられる復号鍵を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の場合に当該装置に前記復号鍵を渡して前記暗号化されたデジタル情報を復号化させるアクセス制御手段を備えていることを特徴とする請求項 1 記載の IC チップ内蔵記録媒体。

【請求項 3】 前記デジタル情報が実行形式のプログラムであり、  
前記 IC チップは、前記実行形式のプログラムの実行に必要な条件情報を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の場合に当該装置に前記条件情報を渡して前記実行形式のプログラムの実行状態を形成させるアクセス制御手段を備えていることを特徴とする請求項 1 記載の IC チップ内蔵記録媒体。

【請求項 4】 前記アクセス制御手段は、前記情報アクセスの際に受信した乱数データの正当性を確認することにより前記認証を行うように構成されていることを特徴とする請求項 2 または 3 記載の IC チップ内蔵記録媒体。

【請求項 5】 コンピュータ装置が読み取り可能なインストール及びインストール対象となるデジタル情報を記録した記録媒体を前記コンピュータ装置に収容可能な形状の筐体に収容するとともに、該筐体の所定部位に、指令入力を契機に認証を行い、認証結果を出力する IC チップを備えた IC チップ内蔵記録媒体であって、前記インストーラが、

前記 IC チップに所定の認証データに基づく認証指令を送出するとともに当該 IC チップから前記認証結果を取得し、認証結果が肯定的の場合に前記 IC チップに記録された前記デジタル情報をインストールする処理を前記コンピュータ装置に実行させるものであることを特徴とする IC チップ内蔵記録媒体。

【請求項 6】 前記デジタル情報が暗号化されたデジタル情報であり、  
前記 IC チップは、前記暗号化されたデジタル情報の復号化に用いられる復号鍵を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の

場合に前記復号鍵を渡すように構成されており、前記インストーラは、前記暗号化されたデジタル情報を前記復号鍵で復号化しインストールする処理を前記コンピュータ装置に実行させるものであることを特徴とする請求項 5 記載の IC チップ内蔵記録媒体。

【請求項 7】 前記 IC チップは、前記認証指令の入力を契機に参照鍵を生成する鍵生成手段と、生成された参照鍵と前記復号鍵とを照合する照合手段とを備え、両鍵が合致したときに肯定的な認証結果を出力することを特徴とする請求項 2 または 6 記載の IC チップ内蔵記録媒体。

【請求項 8】 前記 IC チップは、前記インストールの回数を計数するインストール回数計数手段と、該インストール回数計数手段による計数値が所定値を越えたときに前記インストールを制限する手段とを備えていることを特徴とする請求項 6 記載の IC チップ内蔵記録媒体。

【請求項 9】 デジタル情報及びこのデジタル情報のインストーラを記録した記録媒体を筐体内に収容するとともに、該筐体の所定部位に IC チップが固定された IC チップ内蔵記録媒体への情報アクセスを行う装置であって、

前記筐体の収容時に前記 IC チップとの間で情報の授受を行うリーダーライタと、  
前記リーダーライタを通じて前記 IC チップに認証指令を送出するとともに該 IC チップからの認証結果が肯定的の場合に前記記録媒体から前記インストーラを読み込んで前記デジタル情報をインストールする制御手段とを有することを特徴とする情報アクセス装置。

【請求項 10】 前記記録媒体には暗号化されたデジタル情報が記録され、前記 IC チップには前記暗号化されたデジタル情報を復号化する復号鍵が保持されており、前記制御手段は、前記認証結果が肯定的の場合に前記 IC チップに格納された復号鍵を用いて前記暗号化されたデジタル情報を復号化した後に前記インストールを行うように構成されていることを特徴とする請求項 9 記載の情報アクセス装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、コンピュータプログラムを記録するためのパッケージ型の記録媒体、例えばフレキシブルディスク (FD)、コンパクトディスク型 ROM (CD-ROM)、光磁気ディスク (MO ディスク)、ミニディスク (MD) と、これらの記録媒体へのアクセスを行うアクセス装置に関し、特に、記録媒体に記録されるコンピュータプログラムのセキュリティを確保する手法に関する。

## 【0002】

【従来の技術】コンピュータプログラムやデータ、コンテンツ等のデジタル情報を流通させる場合、これらをコンピュータ読み取り可能な形態でパッケージ型の記録媒

体に記録することがよく行われている。ユーザは、この記録媒体をコンピュータ装置にセットし、インストールして使用できるようにする。しかし、従来、記録媒体には記録情報のセキュリティ対策が十分に施されていないため、不正コピーを防ぐための対策は貧弱である。

【0003】例えば購入者から記録媒体を借用した第三者が、デジタル情報を自分のコンピュータ装置へインストールすることはきわめて容易である。ソフトウェアID番号付与やユーザ登録制なども試みられているが、不正コピー防止の根本的な解決には結びつかないのが現状である。なお、記録情報の同一性を保持する手段として、例えばFDの場合には、パッケージのスライドスイッチを「書き込み不可」に設定することはよく行われることであるが、この「書き込み不可」の状態を「書き込み可能」の状態に変更することは極めて容易であり、セキュリティと呼ぶには至らない。

#### 【0004】

【発明が解決しようとする課題】近年、記録対象となるデジタル情報のサイズは肥大化しており、それに対応して、記録媒体も、CD-ROMのような、読み取り専用ではあるが、大容量の記録媒体が使用されている。しかし、このような記録媒体は、製造工程の都合上、媒体毎のソフトウェアID番号の付与は行われていない。通常、プログラム等のインストールの際には、ソフトウェアID番号を入力することが必要となるが、多くの場合、このソフトウェアID番号が記録媒体に記録されているわけではなく、ソフトウェアID番号をハッシュ関数にかけた結果が予め記録媒体内に保存されたテーブルにあれば、インストールできるようになっている。例えばA氏の購入した記録媒体のソフトウェアID番号で、B氏の購入した同じ記録媒体の記録情報のインストールが可能となる。このように同じ記録媒体から何度でもインストールできる事態は好ましくなく、デジタル情報のセキュリティを図るための技術開発が望まれていた。

【0005】そこで本発明は、ICチップの耐タンパ性と高セキュリティ性とを利用して、記録されたデジタル情報のセキュリティを確保するICチップ内蔵記録媒体を提供することを課題とする。本発明の他の課題は、ICチップ内蔵記録媒体への情報アクセスを行う情報アクセス装置を提供することにある。

#### 【0006】

【課題を解決するための手段】上記課題を解決する本発明のICチップ内蔵記録媒体は、記録媒体に記録されたデジタル情報の読み取り及びICチップへの情報アクセスとを行う装置に収容可能な形状の筐体を有するもので、該筐体の内部には前記記録媒体が収容され、所定部位には前記ICチップが取り付けられており、前記ICチップは、前記装置による前記デジタル情報の読み取りを規制するように構成されていることを特徴とする。

【0007】前記デジタル情報は、例えば所定の暗号ア

ルゴリズムで暗号化されたデジタル情報とする。この場合、前記ICチップは、前記暗号化されたデジタル情報の復号化に用いられる復号鍵を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の場合に当該装置に前記復号鍵を渡して前記暗号化されたデジタル情報を復号化させるアクセス制御手段を備えるようにする。

【0008】前記デジタル情報は、実行形式のプログラムであってもよい。この場合、前記ICチップは、前記実行形式のプログラムの実行に必要な条件情報を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の場合に当該装置に前記条件情報を渡して前記実行形式のプログラムの実行状態を形成させるアクセス制御手段を備えるようにする。条件情報は、例えば起動情報、鍵情報、あるいはプログラムの実行手順を定めたデータである。

【0009】前記アクセス制御手段は、例えば、前記情報アクセスの際に受信した乱数データの正当性を確認することにより前記認証を行うように構成される。

【0010】本発明の他のICチップ内蔵記録媒体は、コンピュータ装置が読み取り可能なインストーラ及びインストール対象となるデジタル情報を記録した記録媒体を前記コンピュータ装置に収容可能な形状の筐体に収容したものである。該筐体の所定部位には、指令入力を契機に認証を行い、認証結果を出力するICチップを備えている。前記インストーラは、前記ICチップに所定の認証データに基づく認証指令を送出するとともに当該ICチップから前記認証結果を取得し、認証結果が肯定的の場合に前記ICチップに記録された前記デジタル情報をインストールする処理を前記コンピュータ装置に実行させるものである。

【0011】このようなICチップ内蔵記録媒体において、前記デジタル情報は暗号化されたデジタル情報であってもよい。この場合、前記ICチップは、前記暗号化されたデジタル情報の復号化に用いられる復号鍵を保持するとともに、前記装置からの情報アクセスの認証を行い、認証結果が肯定的の場合に前記復号鍵を渡すように構成し、前記インストーラは、前記暗号化されたデジタル情報を前記復号鍵で復号化してインストールする処理を前記コンピュータ装置に実行させるようにする。

【0012】なお、前記ICチップが復号鍵を保持する場合は、前記認証指令の入力を契機に参照鍵を生成する鍵生成手段と、生成された参照鍵と前記復号鍵とを照合する照合手段とをさらに備え、両鍵が合致したときに肯定的な認証結果を出力するように構成する。

【0013】好ましくは、前記ICチップが、さらに、前記インストールの回数を計数するインストール回数計数手段と、該インストール回数計数手段による計数値が所定値を越えたときに前記インストールを制限する手段とを備えるようにする。

【0014】上記他の課題を解決する本発明の情報アクセス装置は、デジタル情報及びこのデジタル情報のインストーラを記録した記録媒体を筐体内に收容するとともに、該筐体の所定部位にICチップが固定されたICチップ内蔵記録媒体への情報アクセスを行う装置であって、前記筐体の收容時に前記ICチップとの間で情報の授受を行うリーダライタと、前記リーダライタを通じて前記ICチップに認証指令を送出するとともに該ICチップからの認証結果が肯定的の場合に前記記録媒体から前記インストーラを読み込んで前記デジタル情報をインストールする制御手段とを有することを特徴とする。

【0015】前記記録媒体に暗号化されたデジタル情報が記録され、前記ICチップに前記暗号化されたデジタル情報を復号化する復号鍵が保持されている場合、前記制御手段は、前記認証結果が肯定的の場合に前記ICチップに格納された復号鍵を用いて前記暗号化されたデジタル情報を復号化した後に前記インストールを行うように構成する。

【0016】

【発明の実施の形態】以下、本発明のICチップ内蔵記録媒体と、本発明の情報アクセス装置とを備えて構成されるコンピュータシステムの実施の形態を説明する。ここでは、デジタル情報を記録する記録媒体をCD-ROMとし、デジタル情報は所定の暗号アルゴリズムで暗号化されているものとする。以下、平文のデジタル情報を単にファイル、暗号化されたファイルを暗号化ファイルと称する。

【0017】図1は、本実施形態によるコンピュータシステムの構成図である。このコンピュータシステムは、ICチップ12を有するICチップ内蔵CD-ROM（以下、IC-CD）10と、IC-CD10のCD-ROM11に記録されたファイルまたは暗号化ファイルをインストールするための情報アクセス装置20とを備えて構成される。

【0018】情報アクセス装置20は、CD-ROM11に記録された情報の読込を行う読込ヘッド21と、ICチップ12との間で情報の授受を行うリーダライタ22とを備え、さらに、装置内部のCPU（図示省略）が所定の制御プログラムを読み込むことにより実現される制御装置23と、補助記憶装置である大容量のハードディスク24とを少なくとも有する。通常、この情報アクセス装置20は、パーソナルコンピュータやワークステーションで実現される。

【0019】IC-CD10は、情報アクセス装置20のメディア装着機構（図示省略）に装着可能な形状、寸法の樹脂製の筐体13内にCD-ROM11を收容するとともに、筐体13の所定部位、すなわちにリーダライタ22に対応する筐体正面部にICチップ12を取り付けたものである。筐体13には、スライド自在のカバー14が取り付けられ、IC-CD10がメディア装着機

構に装着されたときに、カバー14がスライドしてCD-ROM11の記録面が露出し、読込ヘッド21がCD-ROM11の記録情報を読み込めるようになっている。

【0020】ICチップ12には、少なくともROM15、RAM16、EEPROM17、CPU18、I/Oポート19が形成されている。

【0021】ROM15には、CPU18によって読み取られて実行されるIC用プログラムが格納されている。RAM16はCPU18によって使用される作業領域であり、EEPROM17には、鍵格納領域171、インストール回数格納領域172、鍵生成回数格納領域173が形成されている。CPU18は、関数演算や入出力制御を行う論理演算プロセッサである。I/Oポート19は、リーダライタ22との間の情報の入出力ポートである。

【0022】本実施形態では、CD-ROM11に、上記暗号化ファイルのほかに、暗号アルゴリズムの情報、インストーラを記録しておく。情報アクセス装置20の側では、IC-CD10がメディア装着機構に装着されたときに、CD-ROM11に記録されたインストーラを読み込み、CPUがそれを実行することにより、種々の機能ブロックを装置内に形成する。ICチップ12においても、CPU18がIC用プログラムを読み込んで実行することにより、種々の機能ブロックを形成する。

【0023】図2は、これらの機能ブロックの相関図である。すなわち、情報アクセス装置20には、乱数処理部26、復号部27、メモリ制御部28の機能ブロックを形成する。乱数処理部26は、図示しない入力装置を通じてユーザの認証データ（乱数）を受け付け、これをリーダライタ22を通してICチップ12に出力するのである。復号部27は、ICチップ12から復号鍵が送られたときにCD-ROM11に記録された暗号化ファイルを復号するものである。メモリ制御部28は、復号化されたファイルをハードディスク24に格納するための制御を行うものである。

【0024】一方、ICチップ12には、メモリ制御部121、鍵生成部122、照合部123、回数検出部124の機能ブロックを形成する。メモリ制御部121は、EEPROM17内の情報の記録制御及び再生制御を行うものであり、鍵生成部122は、上記乱数処理部26から入力される乱数に基づいて参照鍵を生成するのである。照合部123は、鍵生成部122で生成された参照鍵がEEPROM17内の鍵格納領域171に格納されている鍵と合致するかどうかを照合し、この照合結果と、インストール回数格納領域172に格納されたインストール可能回数を参照してインストールの可否をリーダライタ22を通じて復号部27に出力するのである。回数検出部124は、インストール回数格納領域172内のインストール回数を更新するものである。

【0025】IC-CD10に記録される暗号化ファイルは、例えば公知の共通鍵方式で暗号化される。この場合の暗号化処理の手順を示したのが図3である。まず、CD-ROM10にファイルを記録する記録装置（図示省略）において、乱数を発生させ（ステップS101）、この乱数と鍵生成関数とを用いて、暗号鍵を生成する（ステップS102）。例えば、鍵生成関数をG(x)、乱数をRとすると、暗号鍵Kは、下記(1)式で求められる。 $K = G(R) \cdots (1)$

【0026】次に、暗号鍵Kと共通暗号アルゴリズムCとを用いて、対象となるファイルF0を暗号化する。これにより生成される暗号化ファイルF1は、下記(2)式により求めることができる（ステップS103）。 $F1 = C(F0) \cdots (2)$

【0027】記録装置は、このようにして生成された暗号化ファイルF1を、共通暗号アルゴリズムC、インストーラと共にCD-ROM11に記録する。また、ICチップ12の鍵格納領域171、インストール回数格納領域172、鍵生成関数格納領域173に、それぞれ暗号鍵K、インストール可能回数の初期値、鍵生成関数G(x)を記録する。ユーザに対しては、IC-CD10と暗号鍵Kの生成に用いられた乱数Rとを配送する。

【0028】次に、コンピュータシステムにおいて、ユーザが、IC-CD10に記録された暗号化ファイルF1を情報アクセス装置20にインストールする場合の手順を、図4に従って説明する。

【0029】乱数RとIC-CD10とを受け取ったユーザがメディア装着機構にIC-CD10を装着すると、情報アクセス装置20は、CD-ROM11に記録されたインストーラを読み込んで実行する（ステップS201）。その後、乱数処理部26でユーザからの乱数Rの入力を受け付け、これを認証指令として、ICチップ12の鍵生成部122に出力する（ステップS202）。鍵生成部122は、EEPROM17の鍵生成関数格納領域173に格納されている鍵生成関数G(x)をメモリ制御部121を介して受け取り、参照鍵を生成する（ステップS203）。

【0030】照合部123は、インストール回数格納領域172に格納されているインストール可能回数Nが“1”以上であり、且つ、鍵格納領域171に予め格納されている鍵と鍵生成部122で生成した参照鍵とを照合する（ステップS204）。両者が合致する場合は（ステップS204; Yes）、回数検出部124に対して肯定的な認証結果、すなわち「OK判定」を送信するとともに、復号部27に対してこの「OK判定」と復号鍵とを送信する。

【0031】回数検出部124は、インストール可能回数Nを“N-1”に更新するとともに、これをメモリ制御部121を介してインストール回数格納領域172に格納する（更新する）（ステップS205）。

【0032】情報アクセス装置20では、復号部27において、復号鍵と共通暗号アルゴリズムCに基づいて暗号化ファイルF1を復号化し、これをメモリ制御部28に出力する（ステップS206）。メモリ制御部28は、復号化後のファイルをハードディスク24にインストールし（ステップS207）、処理を終了させる。一方、ステップS204において、参照鍵と復号鍵が合致しなかった場合、あるいはインストール可能回数Nが“0”であった場合（ステップS204; No）、照合部123は、復号部27に否定的な認証結果、すなわち「NG判定」を送信する。このNG判定を受信した復号部27は、直ちに処理を終了させる。

【0033】このように、暗号化ファイルF1をCD-ROM11に記録し、復号鍵等をICチップ12に保持させることにより、CD-ROM11に記録された情報のアクセス制御をICチップ12に任せることが可能になる。例えば、従来のCD-ROMやFD等では不可能であった、ユーザの正当性の認証やインストール回数の制限を行うことが可能になり、ファイルのセキュリティ対策が万全となる。

【0034】なお、本実施形態では、記録媒体として、筐体13に格納されたいわゆるパッケージ型のCD-ROMを例に挙げて説明したが、ICチップを固定できる構造の他の記録媒体、例えばMOやDVD等にも同様に本発明を適用できるものである。

【0035】

【実施例】次に、上記IC-ID10の実施例を説明する。

（第1実施例）上記IC-ID10を用いることにより、アプリケーション処理の分散化を行うことが可能である。つまり、所定のアプリケーション処理を実行するためのファイルのうち、実行形式のプログラムの部分だけをCD-ROM11に記録してインストールの対象ファイルとし、ICチップ12には上記プログラム用のバッチ・モジュール等を搭載し、両者を組み合わせて一つのアプリケーション処理を実行できるようにすることも可能である。このように、アプリケーション処理の分散化を行うことにより、インストール時のメモリ容量を低減させることができるようになる。

【0036】（第2実施例）また、CD-ROM11に実行形式のプログラムを記録するとともに、ICチップ12（EEPROM17）にそのプログラムの実行に必要な条件情報を更新自在に記録できるようにし、これらを情報アクセス装置20において合体させることで、必ずしもインストールすることなく、IC-CD10のみで上記プログラムを実行できるようにする形態も可能である。

【0037】この場合の実行形式のプログラムの例としては、例えばRPG（ロールプレイングゲーム）等のゲームプログラム、ビジネス用AP（APは、アプリケー

ション・プログラム、以下同じ)、電子マネー用AP等が挙げられる。また、ICチップ12に記録される条件情報としては、ゲームプログラムの場合はプレイヤー毎のゲーム進行情報その他の可変情報、ビジネス用APの場合はデータ、電子マネー用APの場合は電子マネー情報となる。各プログラムの起動に必要なコンピュータ装置の環境情報や鍵情報としてもよい。

【0038】このような使用形態を採用することにより、実行形式のプログラムと一緒に条件情報を持ち歩き、プログラム実行時に両者を合体させてIC-CD 10上から起動させることができるので、複数のプログラムの実行環境の競合を防止できるようになる。

【0039】情報アクセス装置20にインストールする必要がある場合でも、プログラムとその条件情報とが一体化されているので、APと条件情報とを別々にコンピュータ装置に移動させる必要がなくなるので、プログラムの実行環境の形成の便宜を図ることができる。

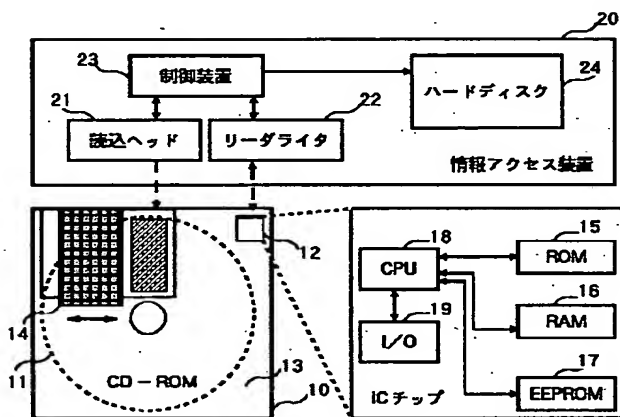
【0040】

【発明の効果】以上の説明から明らかなように、本発明のICチップ内蔵記録媒体によれば、記録されたデジタル情報や、デジタル情報の配送時のセキュリティが万全となり、不正コピーの防止のみならず、ライセンスパッケージ等をソフトウェアメーカーの関与なしに行うことが可能になる、という特有の効果が得られる。

【図面の簡単な説明】

【図1】本発明を適用したコンピュータシステムの一実施の形態を示す構成図。

【図1】



\* 【図2】本実施形態による機能ブロックの相関図。

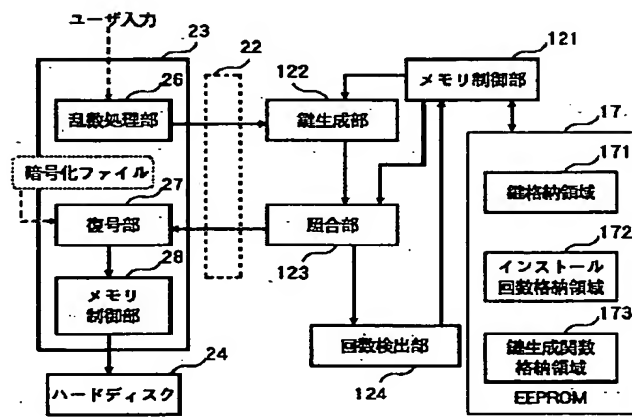
【図3】本実施形態による記録対象ファイルの暗号化手順を示した説明図。

【図4】本実施形態による記録対象ファイルのインストールの手順説明図。

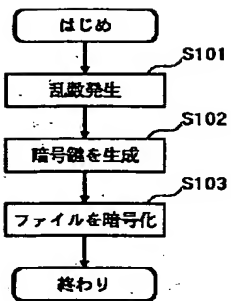
【符号の説明】

- 10 IC-CD
- 11 CD-ROM
- 12 ICチップ
- 13 筐体
- 14 カバー
- 17 EEPROM
- 18 CPU
- 20 情報アクセス装置
- 21 読込ヘッド
- 22 リーダライタ
- 23 制御装置
- 24 ハードディスク
- 26 乱数処理部
- 27 復号部
- 28, 121 メモリ制御部
- 122 鍵生成部
- 123 照合部
- 124 回数検出部
- 171 鍵格納領域
- 172 インストール回数格納領域
- 173 鍵生成回数格納領域

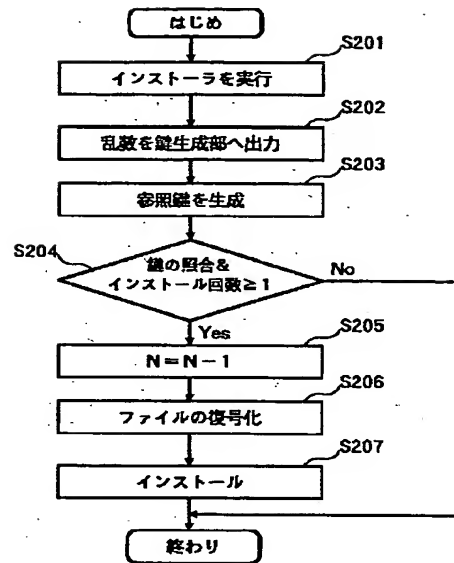
【図2】



【図3】



【図4】



フロントページの続き

(51) Int. Cl.<sup>6</sup>

G 0 6 F 12/14

G 1 1 B 7/24

19/04

識別記号

3 2 0

5 7 1

5 0 1

F I

G 0 6 F 12/14

G 1 1 B 7/24

19/04

3 2 0 E

5 7 1 A

5 7 1 Z

5 0 1 H